Министерство внутренних дел Российской Федерации

Главное управление вневедомственной охраны

УТВЕРЖДЕНО
Заместителем начальника
ГУВО МВД России
генерал-майором полиции
А.В. Грищенко

«25» 12 2015 года

# Применение оборудования с использованием защищенных каналов передачи данных, предоставляемых операторами сотовой связи

## Методические рекомендации

Начальник ФКУ НИЦ «Охрана»
МВД России
полковник полиции
А.Г. Зайцев

«18» 12 2015 года

2015

gost.e-ecolog.ru

*Методические рекомендации разработаны сотрудниками Федерального казённого учреждения «Научно-исследовательский центр «Охрана» Министерства внутренних дел Российской Федерации к.т.н. А.А. Никитиным, к.т.н. А.Р. Фамильновым, И.М. Нурмухаметовым, А.А. Клочковым, Г.М. Деминым под руководством к.т.н. А.Г. Зайцева и утверждены Главным управлением вневедомственной охраны Министерства внутренних дел Российской Федерации.*

***Применение оборудования с использованием защищенных каналов передачи данных, предоставляемых операторами сотовой связи. Методические рекомендации. – М.: НИЦ «Охрана» – 26 с.***

В методических рекомендациях рассмотрены вопросы применения защищенных каналов передачи данных, предоставляемых операторами сотовой связи, в целях организации централизованной охраны.

Приведены необходимые сведения для подразделений вневедомственной охраны полиции по организации предлагаемых схем использования оборудования технических средств охраны, список оборудования, имеющего возможность работы со специализированными сотовыми каналами связи, а также общие рекомендации по настройке оборудования пультов централизованного наблюдения, описание возможностей специализированных веб - приложений.

Методические рекомендации предназначены для инженерно-технических специалистов вневедомственной охраны, занимающихся вопросами организации централизованной охраны объектов, квартир и мест хранения имущества граждан.

**ВВЕДЕНЫ**
С «__» _____ 2016 г.

**© ФКУ НИЦ «Охрана» МВД России, 2016**

## 1. ВВЕДЕНИЕ

В настоящее время на отечественном рынке широко представлены системы и устройства охранной сигнализации, использующие сотовые каналы связи для передачи данных от охраняемых объектов на ПЦН.

Применение каналов сотовой связи в системах централизованного наблюдения обусловлено возможностью осуществления беспроводного подключения объектового оборудования на нетелефонизированных объектах при их широком территориальном охвате.

При тех преимуществах, которые дает использование данных каналов связи, необходимо учитывать определенные факторы, негативно влияющие на надежность доставки тревожной и служебной информации от охраняемых объектов:

- использование сети общего доступа, что не обеспечивает защиту от несанкционированного вмешательства и от естественных «перегрузок» сети;

- используемые методы передачи данных (в основном это SMS, Contact ID) не обеспечивают требуемую скорость и надёжность доставки тревожной информации;

- подверженность канала связи влиянию естественных и преднамеренных помех;

- уязвимость оборудования сотовой связи к умышленному подавлению;

- отсутствие или сложность организации контроля канала связи.

В настоящее время ведущие операторы сотовой связи активно внедряют новые технологии передачи информации с высоким уровнем защиты, предназначенные для автоматизации банковских операций и бизнес-процессов.

В интересах подразделений вневедомственной охраны предлагается использование аналогичных технологий на основе защищенного беспроводного

доступа в корпоративных сетях по каналам GPRS/EDGE, 3G, LTE для подключения объектового и пультового оборудования технических средств охраны.

Целью настоящих рекомендаций является доведение необходимой информации до специалистов подразделений вневедомственной охраны по организации централизованной охраны с использованием указанных каналов.

## 2. ОПРЕДЕЛЕНИЯ И УСЛОВНЫЕ СОКРАЩЕНИЯ

В настоящих рекомендациях приняты следующие определения:

**Сеть GSM** – международный стандарт цифровой сотовой связи, глобальная система мобильной связи. Сеть GSM состоит из нескольких функциональных единиц, чьи функции и интерфейсы специфицированы. Сеть состоит из трех частей: мобильный телефон, который находится у абонента; базовая станция, которая контролирует радиосвязь с мобильным телефоном; сетевая подсистема, основной частью которой является центр коммутации, выполняющий коммутацию вызовов между мобильными абонентами или между мобильными абонентами и абонентами фиксированных сетей;

**Сеть VPN** – виртуальная частная сеть (Virtual Private Network, Virtual Private Net) – это объединение локальных сетей или отдельных машин, подключенных к сети общего пользования, в единую сеть, обеспечивающую секретность и целостность передаваемой по ней информации;

**IP-адрес** – уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP;

**Статический IP-адрес** – IP-адрес называют статическим (постоянным, неизменяемым), если он прописывается в настройках устройства пользователем, либо если назначается автоматически при подключении

устройства к сети, но используется в течение неограниченного промежутка времени и не может быть присвоен другому устройству;

**Динамический IP-адрес** – IP-адрес называют динамическим (непостоянным, изменяемым), если он назначается автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, как правило, до завершения сеанса подключения;

**Маршрутизатор (роутер)** – совокупность аппаратных и программных средств для управления потоком данных в сети;

**Межсетевой экран (файервол, брандмауэр)** — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

**Шлюз** - устройство, конвертирующее сигналы/данные в форму, пригодную для транспортировки по сети Интернет;

**SIM-карта** – смарт-карта, применяемая в мобильных телефонах, содержит идентификаторы пользователя, необходимые для доступа к сети.

В настоящих рекомендациях приняты следующие сокращения:

АРМ – автоматизированное рабочее место

МХИГ – место хранения имущества граждан

ПО – программное обеспечение

ПЦО – пункт централизованной охраны

ПЦН – пульт централизованного наблюдения

СПИ – система передачи извещений

УОО – устройство оконечное объектовое

| | |
|---|---|
| УОП | – устройство оконечное пультовое |
| ШС | – шлейф сигнализации |
| APN | - Access Point Name, (англ. - имя точки доступа) — шлюз из мобильной сети передачи данных (например, GPRS, 3G), через который осуществляется доступ к услугам передачи данных |
| Contact ID | - распространенный протокол информаторных систем передачи извещений |
| CSD | - Circuit Switched Data — технология передачи данных, разработанная для стандарта GSM. В CSD режиме соединение с удаленным устройством устанавливается по голосовому каналу на скорости до 9,6 кбит/с |
| DNS | - Domain Name System (англ. - служба централизованного разрешения имен) |
| GGSN | - GPRS Gateway Service Node — узел, входящий в состав GPRS Core Network, и обеспечивающий маршрутизацию данных между GPRS Core network (GTP) и внешними IP сетями |
| GPRS | - General Packet Radio Service (англ. - пакетная радиосвязь общего пользования) - услуга пакетной передачи данных по радиоканалу |
| L2TP | - Layer 2 Tunneling Protocol (англ. - протокол туннелирования второго уровня) - в компьютерных сетях туннельный протокол, использующийся для поддержки виртуальных частных сетей. Служит для инкапсуляции кадров протокола PPP в IP-пакеты |
| LTE | *Long-Term Evolution* - стандарт беспроводной высокоскоростной передачи данных |
| SGSN | Serving GPRS Support Node (англ. - узел обслуживания абонентов GPRS) — основной компонент GPRS-системы по реализации всех функций обработки пакетной информации. SGSN выступает точкой соединения между системой базовых станций сети |

радиодоступа и базовой сетью

SMS - Short Message Service (англ. — служба коротких сообщений) — технология, позволяющая осуществлять приём и передачу коротких текстовых сообщений

PPP - Point to Point Protocol - двухточечный протокол канального уровня (Data Link) сетевой модели OSI. Обычно используется для установления прямой связи между двумя узлами сети, причем он может обеспечить аутентификацию соединения, шифрование (с использованием ECP, RFC 1968) и сжатие данных

TCP/IP - Transmission Control Protocol/Internet Protocol (стек для организации составных сетей, которые построены на основе разных сетевых технологий)

## 3. ОБЛАСТЬ ПРИМЕНЕНИЯ

Областью применения данных рекомендаций является организация централизованной охраны в подразделениях вневедомственной охраны с использованием защищённых каналов передачи данных, предоставляемых операторами сотовой связи. В соответствии с методическими рекомендациями Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под централизованную охрану» и Р 78.38.032-2013 «Инженерно - техническая укрепленность и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны» данные предложения предназначены следующих применений:

- организация резервного канала передачи извещений для охраняемых объектов, за исключением объектов категории А1;

- применение оборудования с использованием вышеуказанных каналов связи для организации охраны объектов, квартир и МХИГ категорий Б2, В3 и Г3 без обязательного дублирования канала связи.

В данных рекомендациях приведены необходимые сведения для подразделений вневедомственной охраны по организации предлагаемых схем использования оборудования технических средств охраны, список оборудования, имеющее возможность работы со специализированными сотовыми каналами связи, а также общие рекомендации по настройке оборудования пультов централизованного наблюдения и описание возможностей предоставляемых операторами сотовой связи специализированных веб - приложений.

## 4. СВЕДЕНИЯ О ПРИМЕНЯЕМЫХ ТЕХНИЧЕСКИХ КАНАЛАХ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ КАНАЛОВ СОТОВОЙ СВЯЗИ

В «Список технических средств безопасности, удовлетворяющих требованиям «Единых технических требований к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» включены системы, имеющие оборудование с использованием каналов сотовой связи, выпускаемые отечественными предприятиями. Данные предприятия осуществляют выпуск 26 объектовых устройств для нужд подразделений вневедомственной охраны, 24 из которых имеют возможности настройки для работы со специализированными сотовыми каналами связи (см. таблицу 1).

Таблица 1

| № | Предприятие | Объектовое устройство | Период выпуска | Количество SIM - карт | Возможность работы со специализированными сотовыми каналами связи |
|---|---|---|---|---|---|
| 1 | ООО НПО «Ахтуба-плюс», г. Волжский, Волгоградская обл. | УОО 4G | 03.2009 - по настоящее время | 2 | да |
| | | УОО 6EG | 01.2013 - по настоящее время | 2 | да |
| 2 | ЗАО «АРГУС-СПЕКТР», г. Санкт-Петербург | УОО «Тандем-2М» | 2007 - по настоящее время | 1 | нет |
| | | УОО «Тандем IP-И» исп.1 | Начало 2012 - по настоящее время | 2 | да |
| | | УОО «Тандем IP-И» исп.2 | Начало 2012 - по настоящее время | 2 | да |
| | | ППКОП «Тандем-1» | Начало 2012 - по настоящее время | 1 | да |
| | | УС-18IP | конец 2013 - по настоящее время | 2 | да |
| 3 | ООО «КВАЗАР», г. Ногинск, Московской области | УОО «Лагуна IP/GSM» | с 2014 г | 2 | да |
| 4 | ЗАО НПФ «Интеграл+», г. Казань | БРО-5GSM исп.1 | 01.08.2008 - 01.10.2012 | 2 | да |
| | | БРО-5GSM исп.2 | 01.10.2012 - по настоящее время | 2 | да |
| | | БРО-4GSM+ | 01.04.2013 - по настоящее время | 2 | да |
| 5 | ООО «Проксима», г. Тула | ППКОП S632-2GSM исп. «В» | 2011 - по настоящее время | 2 | да |
| | | ПОО S632-2GSM исп. «В.01» | 2013 - по настоящее время | 2 | да |
| | | ПОО S632-2GSM исп. «В.02» | 2014 - по настоящее время | 2 | да |
| 6 | ЗАО «Риэлта», г. Санкт-Петербург | Заря ГК-IP-М2 | 2009 - по настоящее время | 1 | да |
| | | Заря УО-IP-GPRS | 2009 - по настоящее время | 2 | да |
| 7 | ООО «Охранное бюро Сократ», г. Иркутск | ППКОП 011-8-1-011м | 2013 - По настоящее время | 2 | да |
| | | Приток-А-КОП-02 | 2012 - по настоящее время | 2 | да |
| | | Приток-А-КОП-01 | 2014 - по настоящее время | 2 | да |

| № | Предприятие | Объектовое устройство | Период выпуска | Количество SIM - карт | Возможность работы со специализированными сотовыми каналами связи |
|---|---|---|---|---|---|
| 8 | ООО «Элеста» г. Санкт-Петербург | ППКОП 4GSM | 2008 - по настоящее время | 2 | да |
| | | УОО 4 IP/GPRS | 2013 - по настоящее время | 2 | да |
| | | УОО 5 GPRS 2012 - по настоящее время | 2 | да | |
| | | ГК РИО | 2008 | 2 | да |
| | | ПОИСК ППКОП 24К с ИМ GSM | 2009 - по настоящее время | 2 | да |
| | | ПОИСК ППКОП 8П с ИМ GSM | 2009 - по настоящее время | 2 | да |
| | | УОО 3 GSM | 2007 - по настоящее время | 1 | **нет** |
| | | Конвертор 18кГц-GPRS | 2010 - по настоящее время | 2 | да |

## 5. ОЦЕНКА СТОИМОСТИ ЭКСПЛУАТАЦИИ ЗАЩИЩЕННЫХ КАНАЛОВ СВЯЗИ

В ФКУ НИЦ «Охрана» МВД России ранее проводились лабораторные испытания по возможности применения ряда технических средств охраны отечественных предприятий-изготовителей с использованием защищённых каналов передачи данных, предоставляемых операторами сотовой связи.

В результате анализа трафика передачи данных были выработаны следующие рекомендации:

1) При выборе тарифов для объектового оборудования нужно принимать во внимание, что при установленном периоде посылки тестового сообщения один раз за 30 сек и устойчивом канале связи одному объектовому устройству требуется для передачи информации около 8 Мбайт трафика в месяц. При установке устройства в зоне неуверенного приёма объем требуемого трафика может существенно увеличиться за счёт дополнительной передачи информации для повторного установления соединения. В зависимости от вида тарифа и

региональных различий стоимость передачи 1 Мбайт информации в настоящее время составляет от 3 до 9 рублей.

В настоящее время, ОАО «Вымпелком» предлагает единый тариф по всем субъектам Российской Федерации за обслуживание по технологии «M2M» стоимостью 60 рублей в месяц за каждое абонентское устройство. В данном тарифе предусмотрено округление до 1 Кбайта раз в сутки, бесплатный внутрисетевой роуминг по всей стране и возможность использования общего трафика, что предполагает возможность перераспределения пакетов трафика между SIM-картами.

ОАО «МТС» внедрен тариф «Телематика», по его условиям которого подключения различных пакетов GPRS (от 5 до 90 Мбайт) с фиксированной абонентской платой стоимостью 1 Мбайт трафика составит 2,8 рубля. Порог округления трафика составляет также 1 Кбайт.

ОАО «Мегафон» предлагает услугу «Управление удалёнными объектами», предназначенную для защищенного беспроводного доступа к информации об удаленных объектах, объединенных в технологические сети. Услуга позволяет обеспечить обмен информацией с удаленными объектами по GPRS, SMS и CSD-каналам, включая передачу отчетов, прием команд и осуществление определенных операций. Размер абонентской платы составляет от 95 до 480 рублей (15 Мбайт и 150 Мбайт данных соответственно) в месяц, при этом трафик округляется в 2 Кбайт (средний объем передаваемых данных в течение каждой сессии).

2) При выборе тарифов на услуги оператора связи для сети ПЦО, в общем случае, рекомендуются безлимитные тарифные планы со скоростью не менее 5 Мбит/сек. Средняя стоимость такого подключения составляет около 1000 рублей в месяц.

В настоящее время выбор оператора сотовой связи осуществляется в соответствии с «Методическими рекомендациями по организации

централизованной охраны с использованием GSM-канала связи и проведению установленных законодательством Российской Федерации торгов на предоставление услуг сотовой связи» ГУВО МВД России от 2014 года, в которых отмечено наличие различных подходов подразделений к приобретению, учету и поддержанию баланса SIM-карт (силами УВО (ОВО), заказчика и обслуживающей организации).

В этом же документе указано следующее: «Использование для централизованной охраны SIM-карт, зарегистрированных на УВО (ОВО), дает возможность в рамках контрактных обязательств исключить случаи отключения канала сотовой связи по причине отрицательного баланса, а также повысить эффективность организации технического обслуживания ТСО, работающих по сети GSM. Кроме того, наличие собственных SIM-карт позволяет подразделениям организовать канал передачи извещений для бюджетных организаций, а также объектов, подлежащих обязательной охране полицией, при отсутствии у них возможности финансирования данной статьи расходов».

Вместе с тем, обращено внимание на то, что «в ходе проведения Торгов существует вероятность смены используемого оператора сотовой связи, что повлечет за собой необходимость переконфигурирования подсистемы GSM, переформирования базы данных, а также замены SIM-карт в объектовых и пультовых оконечных устройствах».

Учитывая это, существует необходимость во внесении дополнительных требований для организации централизованной охраны с использованием защищённых каналов передачи данных, предоставляемых операторами сотовой связи.

Поскольку доступ в защищённую сеть предоставляется только зарегистрированным пользователям, следует учитывать, что предлагаемые к использованию каналы связи могут быть реализованы только на

специализированных корпоративных тарифах.

## 6. ОРГАНИЗАЦИЯ РАБОТЫ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ЗАЩИЩЕННЫХ КАНАЛОВ СВЯЗИ.

Для организации предлагаемых схем использования оборудования технических средств охраны, подразделению вневедомственной охраны необходимо через центральные офисы операторов сотовой связи обратиться в региональные отделы, отвечающие за взаимодействие с корпоративными клиентами. Это:

- департамент по работе со стратегическими клиентами или служба продаж телематических сервисов в ОАО «Вымпелком»;

- отдел по реализации специальных программ и взаимодействию с государственными органами в ОАО «Мегафон»;

- департамент по работе с бизнес-рынком или отдел по работе с клиентами крупного бизнеса в ОАО «МТС».

Для применения оборудования подсистем передачи извещений с использованием защищённых каналов, предоставляемыми операторами сотовой связи, предлагаются к использованию со стороны объектового оборудования технологии пакетной передачи данных GPRS/EDGE стандарта GSM (выделенные виртуальные защищённые IP-сети регионального и федерального масштаба, с возможностью предоставления сервисов приоритетного обслуживания) и технология CSD.

Подсистемы не имеют входов и выходов в сеть Интернет, телефонные сети общего доступа и другие сервисы, предлагаемые операторами связи.

Подсистемы обеспечивают уникальность адресного пространства для каждого из пунктов централизованной охраны.

В соответствии с «Едиными техническими требованиями к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» объектовое устройство должно обеспечивать возможность работы не менее, чем с двумя SIM-картами. В целях резервирования канала связи необходимо использование двух SIM-карт в одном объектовом устройстве от различных операторов связи. Для повышения надёжности работы объектового устройства, при сбое в рабочем канале связи, оно переключается на работу с одного оператора связи на другого.

Для осуществления контроля канала между объектовыми устройствами и ПЦН осуществляется передача тестовых извещений, период которых зависит от конкретного типа оборудования и устанавливается при его настройке с учётом того требования, что время обнаружения нарушения связи (неисправность оборудования, естественные или преднамеренные помехи и пр.) не должно превышать 120 секунд.

## 7. ПРИНЦИПЫ ОРГАНИЗАЦИИ УДАЛЕННОГО ДОСТУПА В КОРПОРАТИВНУЮ СЕТЬ КЛИЕНТА ЧЕРЕЗ GPRS/EDGE СЕТЬ ОПЕРАТОРА СОТОВОЙ СВЯЗИ

Для предоставления доступа в корпоративную сеть по каналам GPRS/EDGE, 3G, LTE операторы сотовой связи выдают зарегистрированным пользователям SIM - карты, содержащие специализированные настройки.

Для подключения объектового устройства к сети техническому специалисту подразделения вневедомственной охраны необходимо ввести полученные от оператора связи значения настроек (APN, Login, Password). Ввод этих настроек осуществляется в соответствии с руководством по эксплуатации, входящим в комплект поставки изделия. Настройки вносятся в энергонезависимую память изделия с помощью стандартных средств,

предназначенных для его программирования, как правило, вспомогательной компьютерной программы. По окончании настройки объектовое устройство будет автоматически подключено к сети.

Общая схема организации защищённого подключения к корпоративной сети объектового и пультового оборудования технических средств охраны приведена на рис. 1.

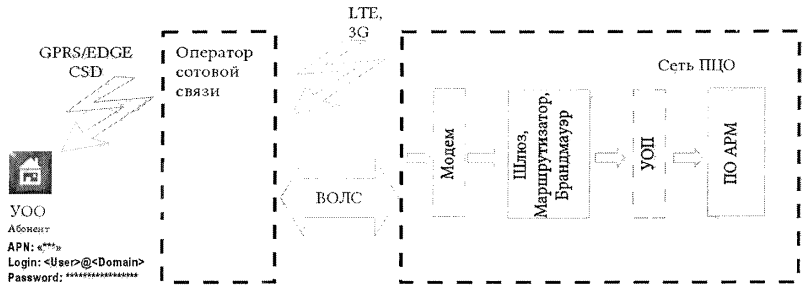



Рисунок 1 - Примерная схема организации защищённого подключения.

В зависимости от типа СПИ с использованием GSM-каналов устройство оконечное пультовое (УОП) может не входить в состав системы (на схеме выделено курсивом). В различных конфигурациях оборудования ПЦН возможны ситуации, когда программное обеспечение (ПО) на автоматизированном рабочем месте (АРМ) будет пытаться найти обновления операционной системы или другого стороннего ПО, и хотя данные сети не имеют доступа в сеть Интернет, запросы существенно повысят трафик. В данном случае необходимо использование межсетевых экранов.

Для организации работы с ПЦН оператор сотовой связи предоставляет физическую выделенную линию с большой пропускной способностью. В качестве резервного канала, а также в случаях ограниченного по времени развертывания системы, рекомендуется использование каналов 3G и/или LTE. В последнем случае, для подключения к сети ПЦО, в настройки модемов 3G

и/или LTE заносятся те же параметры APN, что и в параметры настройки сети объектового устройства.

Получение доступа к IP-сети клиента осуществляется через встроенный GPRS/EDGE-модем, установленный в объектовом устройстве.

Со стороны объектового оборудования связь осуществляется по каналам GPRS/EDGE в основном режиме работы и по каналу CSD - в резервном.

Объектовое устройство устанавливает GPRS сессию с использованием выделенного оператором сотовой связи APN, что позволяет настроить маршрутизацию трафика и направить весь трафик с SIM-карт, минуя публичный Интернет, по выделенному каналу напрямую на сервер клиента. Таким образом существенно повышается защищенность передачи данных.

Для организации и применения вышеуказанных подсистем передачи извещений со стороны ПЦН рекомендуется использование предоставляемых данными операторами выделенных проводных, оптоволоконных, а также беспроводных каналов 3G и LTE. Для повышения надежности канала ПЦО рекомендуется комбинированный тип подключения.

Настройка оборудования ПЦН носит индивидуальный характер и зависит от используемого типа СПИ, возможностей каналов связи, каналообразующего оборудования и пр.

Однако, в настройках сетевого оборудования, установленного на ПЦО, следует использовать отдельно выделенные аппаратные межсетевые экраны с минимальным необходимым набором открытых каналов связи.

В случае, когда оператор сотовой связи физически не может предоставить выделенного проводного или оптоволоконного канала связи, рекомендуется использование VPN согласно схеме на рис.2.

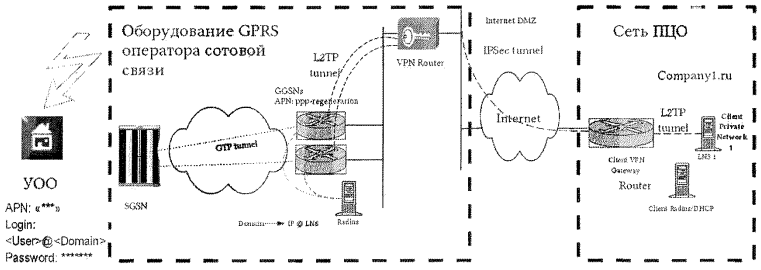



Рисунок 2 - Схема подключения к корпоративной сети GPRS/EDGE с использованием каналов Internet

При приобретении сетевого оборудования необходимо уточнить у оператора связи рекомендуемые и апробированные конкретные модели роутеров с точным указанием версий ПО, обеспечивающие корректную работу с протоколом L2TP.

Шлюз, маршрутизатор и межсетевой экран должны выполняться на отдельном оборудовании. В данном случае наиболее корректно и устойчиво удаётся реализовать функции ограничения доступа, фильтрации пакетов, управления пропускной способностью и пр.

## 8. ОПИСАНИЕ СРЕДСТВ ОПЕРАТИВНОГО УПРАВЛЕНИЯ БЕСПРОВОДНОЙ СВЯЗЬЮ, ПРЕДОСТАВЛЯЕМЫХ ОПЕРАТОРАМИ СОТОВОЙ СВЯЗИ.

При организации доступа к корпоративным защищённым сетям операторы сотовой связи (ОАО «Вымпелком», ОАО «Мегафон», ОАО «МТС») предоставляют также доступ к защищенным веб-приложениям и комплексным пакетам веб-служб, предоставляющим информацию о состоянии и

использовании беспроводных служб связи в реальном времени, а также инструменты для оперативного управления беспроводными устройствами.

При использовании приложений клиенты получают следующие возможности:

- администрирование приложений и пользователей и уровней доступа;

- создание, регистрация и поддержка собственных клиентов для оказания им услуг;

- управление SIM-картами и тарифами;

- просмотр и анализ подробной информации об использовании и выставлении счетов;

- доступ к данным о беспроводных структурах и их анализ в режиме реального времени;

- анализ функционирования и использования SIM-карт;

- получение справочных сведений;

- экспорт данных во внешние приложения (например, в формат *.xls).

Средства оперативного управления беспроводной связью, предлагаемые операторами сотовой связи, имеют единообразные интерфейсы для использования необходимых функций:

- проверка работоспособности канала связи от объектового оборудования;

- контроль за активностью SIM-карт;

- отслеживание израсходованного трафика и финансовых средств;

- переключение между тарифами;

- активация/деактивация SIM-карт;

- экспорт данных для дальнейшей подготовки отчетов.

Получив доступ к интерфейсу платформы, пользователь может в режиме реального времени отслеживать состояние всех его SIM-карт.

Ниже по тексту приведены виды окон, демонстрирующие предоставляемые операторами возможности. Контроль за расходованием финансовых средств группы объектов приведен на рис. 3, а контроль по одному объекту - на рис. 4. Пример контроля активности SIM-карт представлен на рис. 5., а пример интерактивной справки - на рис. 6.

Встроенная система диагностики позволяет определить реальное состояние SIM-карты, что в результате каких-либо проблем поможет определить на каком этапе происходит сбой. Например, увидев, что со стороны оператора все в норме, можно сделать вывод, что проблема с оконечным устройством и наоборот. Отсутствие необходимости отправки ремонтной бригады к устройству (зачастую удаленному или труднодоступному), зная о существовании проблемы со стороны оператора (см. рис. 7).

Для более детальной диагностики платформа располагает функционалом Spotlight, который позволяет определить на каких SGSN и GGSN зарегистрирована SIM-карта, посмотреть параметры GPRS сессии, увидеть все попытки авторизации в сети, факты отправки SMS и статус доставки, наличие «пустых» сессий, когда при поднятой GPRS сессии трафик не передавался. Пример расширенной диагностики приведен на рис. 8.

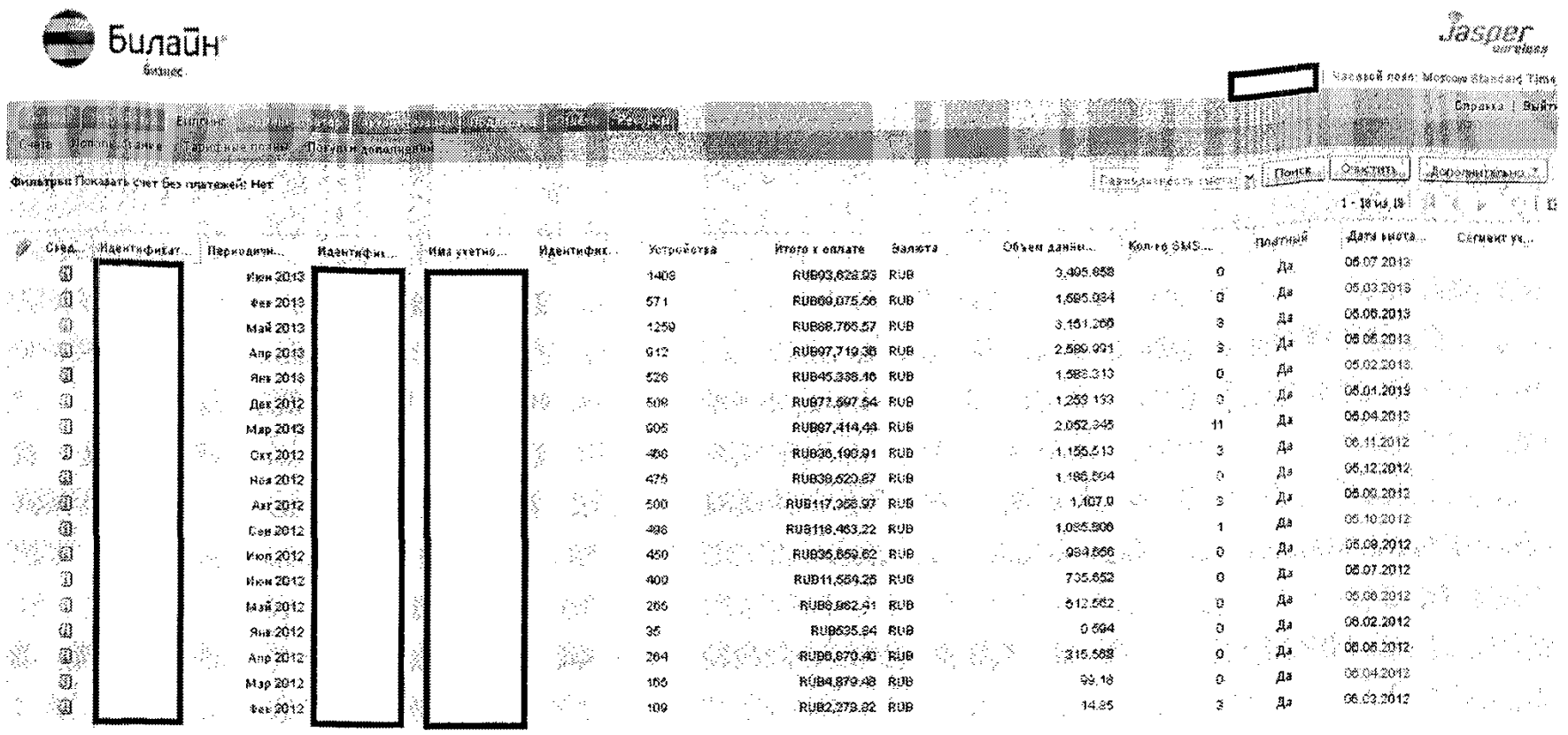



Рис.3. Пример контроля за расходованием финансовых средств группы объектов.

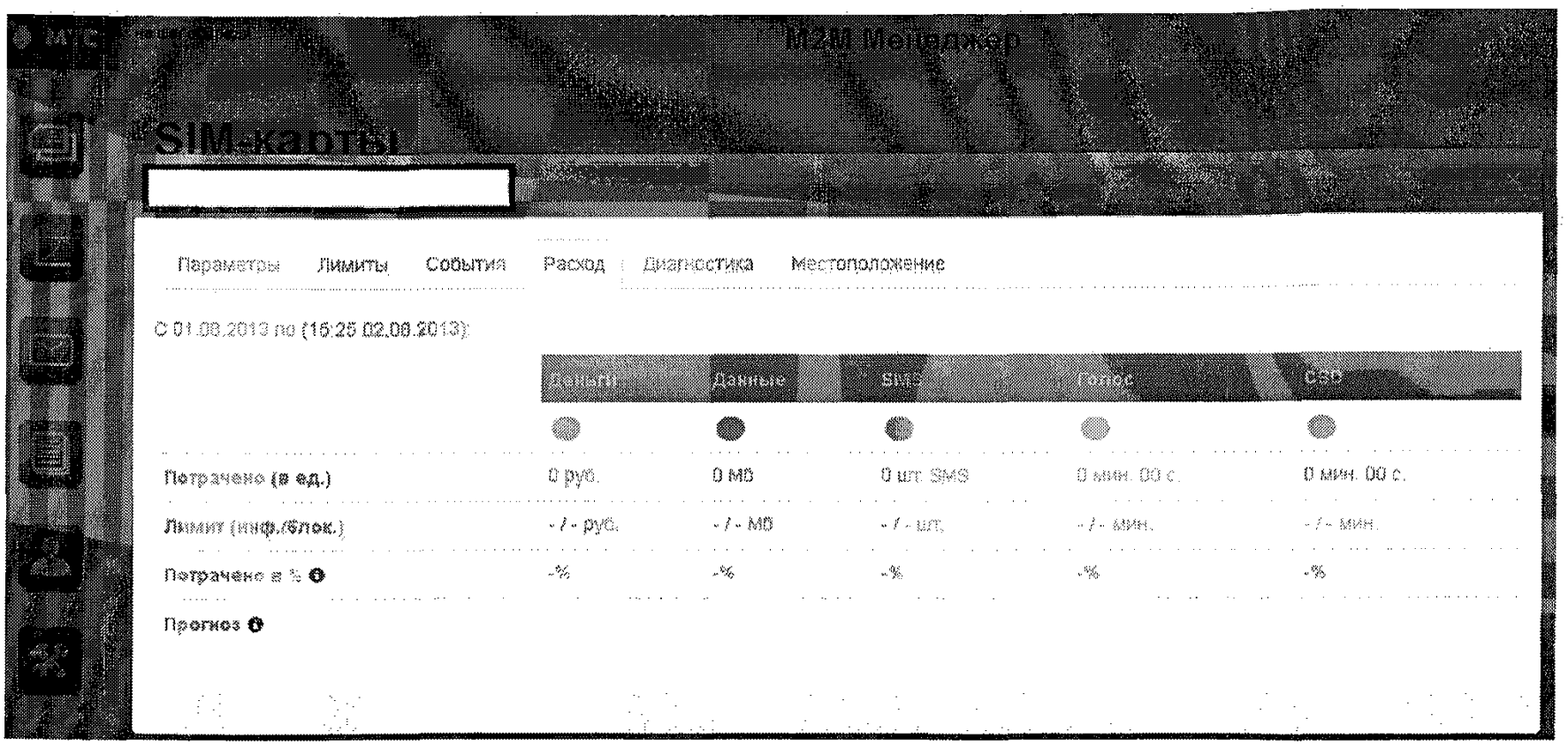



Рис.4. Пример контроля расхода средств по одному объекту.

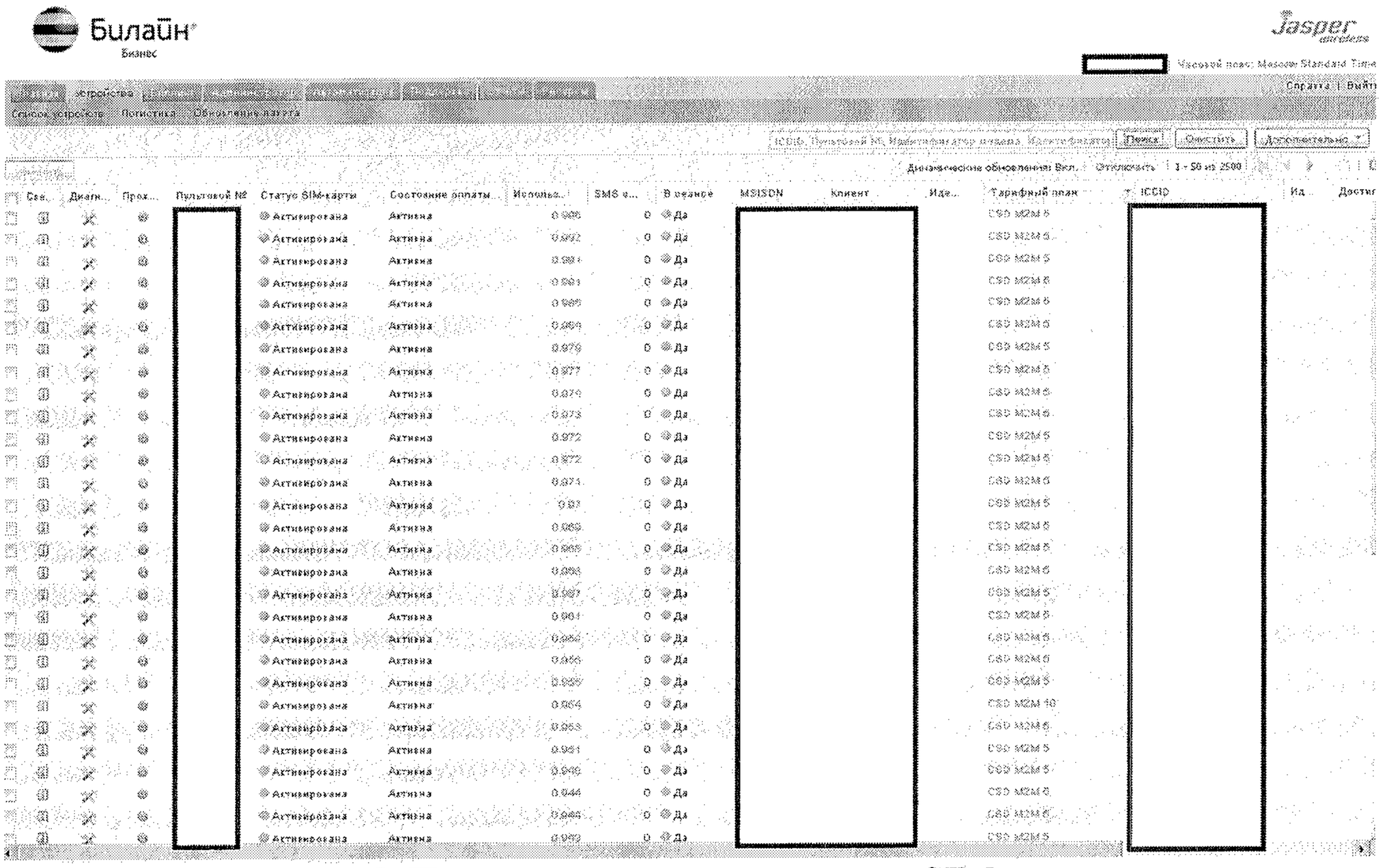



Рис. 5. Пример контроля активности SIM-карт.

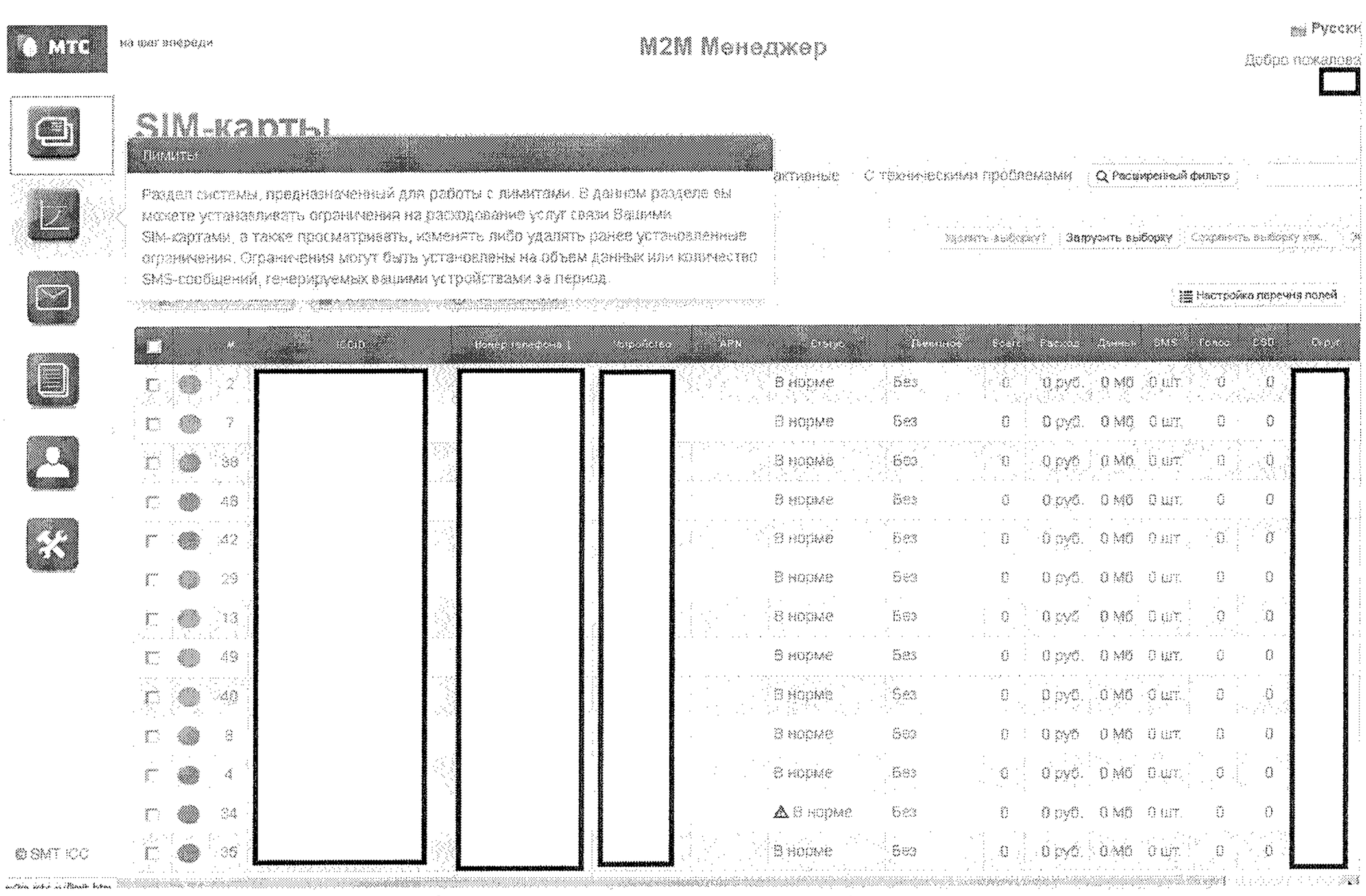
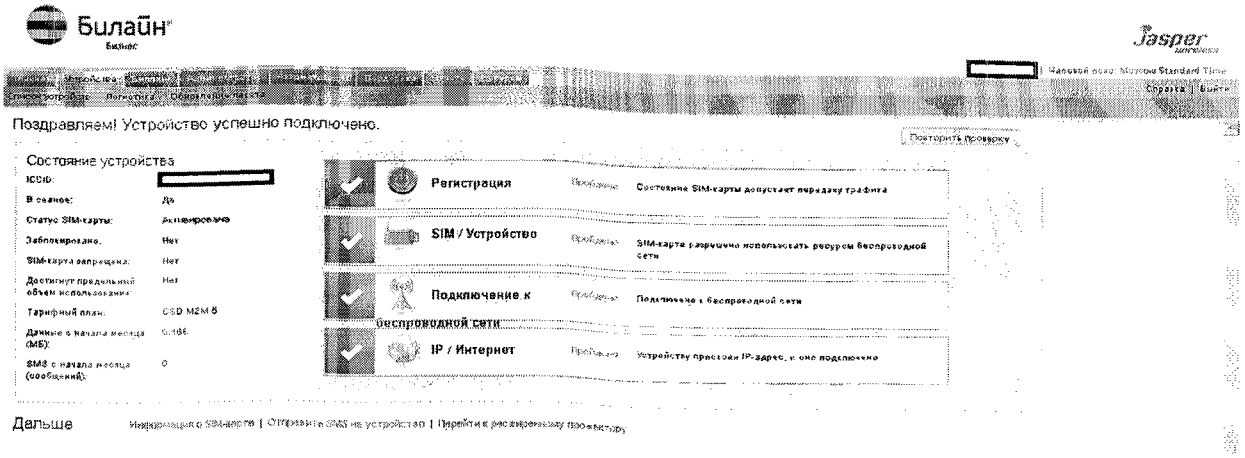
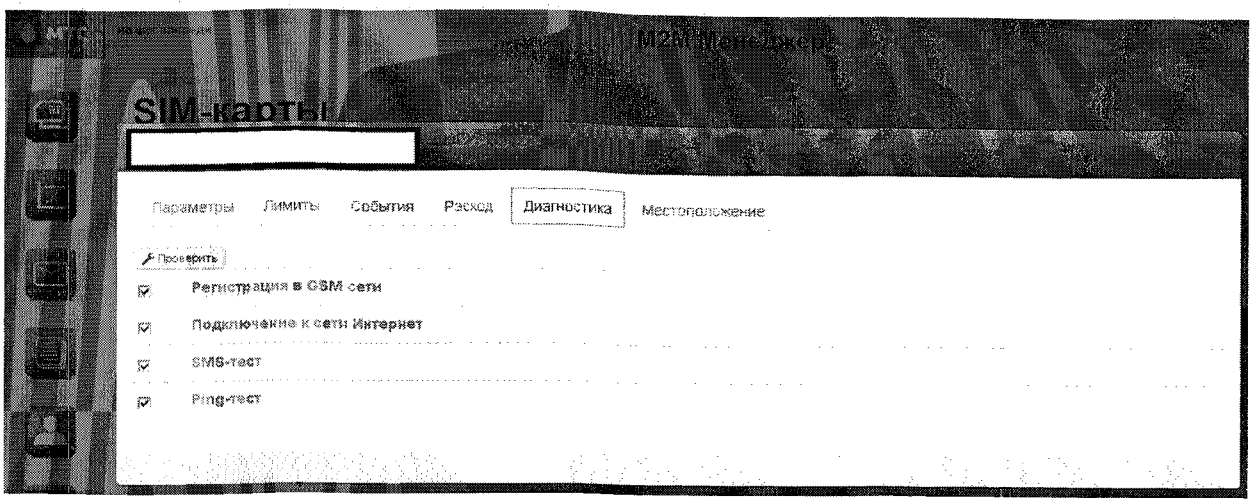



Рис.6. Пример интерактивной справки.




а)




б)

Рис.7. Пример контроля работоспособности канала связи от объектового оборудования.

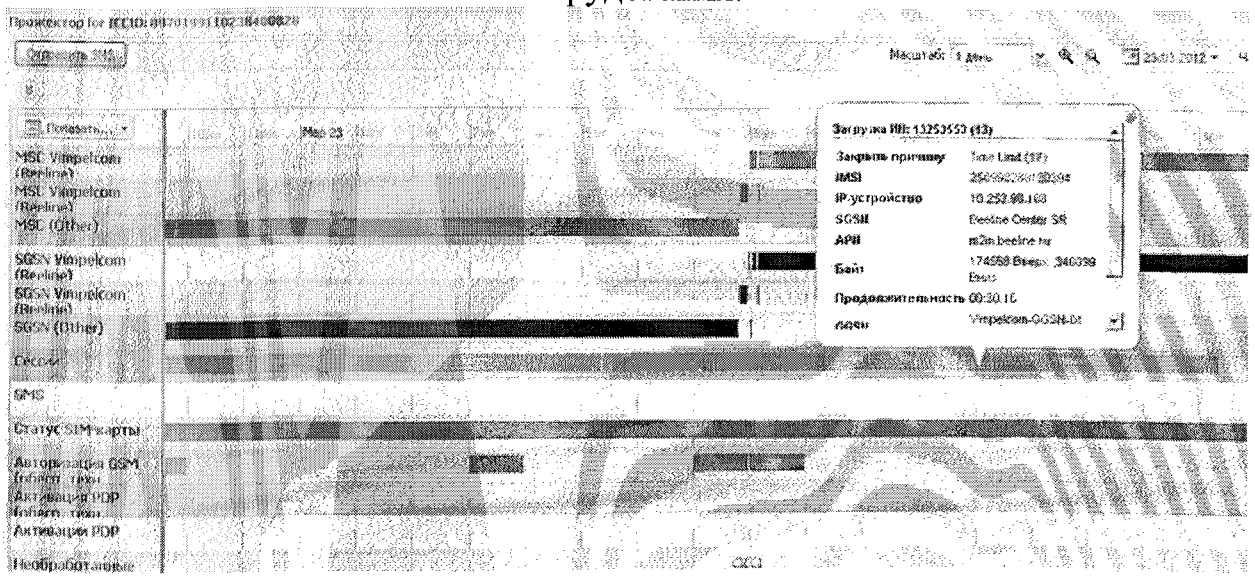



Рис.8. Пример расширенной диагностики канала связи.

## 9. ЗАКЛЮЧЕНИЕ

В настоящее время технические средства охраны с использованием каналов сотовой связи зачастую применяются с морально устаревшими, не обеспечивающими необходимыми уровнями надежности и скорости доставки извещений технологиями (SMS, Contact ID и т. п.). Использование технологий передачи данных SMS, CSD, информаторных протоколов типа Contact ID не позволяет обеспечивать своевременный контроль связи с ПЦН и гарантировать требуемое время доставки тревожных извещений от объектового оборудования до ПЦН и время доставки сигналов управления от ПЦН. Кроме того, при использовании технологии с помощью голосового канала без установления связи возможна доставка только одного тревожного извещения, не обеспечивается необходимая информативность (не передаются сообщения: постановка на охрану, снятие с охраны, неисправность, тест канала связи), отсутствует канал доставки сигналов управления от ПЦН.

Достаточно весомая часть охраняемых объектов, квартир и МХИГ с применением каналов GSM не имеют дублирования по каналам другого оператора сотовой связи или по каналам проводного Интернета.

Использование предлагаемых операторами сотовой связи защищенных каналов связи позволит подразделениям вневедомственной охраны улучшить качество доставки служебной и тревожной информации, а также реализовать ряд преимуществ, к которым относятся:

- обеспечение более высокой степени защиты информации в каналах связи;

- повышение приоритета обслуживания канала связи со стороны операторов сотовой связи;

- возможность управления подключением устройств оконечных к специализированным сетям, предоставляемым операторами сотовой связи;

- оперативное осуществление удаленной диагностики работоспособности канала связи;

- обеспечение возможности анализа расхода трафика, а также изменения подключенных услуг и тарифов;

- возможность контроля наличия денежных средств на каждой SIM-карте, а также пополнения балансового счета для исключения случаев приостановки их обслуживания;

- возможность отказа от использования ненадежных и низкоскоростных протоколов передачи информации;

- возможность заключения соглашений с операторами сотовой связи об использовании корпоративных тарифных планов и экономию денежных средств.

## 10. СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1) Рекомендации Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под централизованную охрану»

2) Методические рекомендации Р 78.38.032-2013 «Инженерно - техническая укрепленность и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны»

3) Методические рекомендации Р 78.36.045-2014 «Защита локальных вычислительных сетей пунктов централизованной охраны при использовании глобальной сети Интернет для передачи данных междуобъектовым и пультовым оборудованием СПИ»

4) «СПИСОК технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны»

5) «Методические рекомендации по организации централизованной охраны с использованием GSM-канала связи и проведению установленных законодательством Российской Федерации торгов на предоставление услуг сотовой связи» ГУВО МВД России от 2014 года

6) Материалы и публикации в интернете, предоставленные ОАО «Мегафон», ОАО «МТС» и ОАО «Вымплелком»

Содержание

1. Введение ..... 3

2. Определения и условные сокращения ..... 4

3. Область применения ..... 7

4. Сведения о применяемых технических каналах связи с использованием каналов сотовой связи ..... 8

5. Оценка стоимости эксплуатации защищенных каналов связи ..... 10

6. Организация работы систем с использованием защищенных каналов связи. 13

7. Принципы организации удаленного доступа в корпоративную сеть клиента через GPRS/EDGE сеть оператора сотовой связи ..... 14

8. Описание средств оперативного управления беспроводной связью, предоставляемых операторами сотовой связи. ..... 17

9. Заключение ..... 23

10. Список используемой литературы ..... 25

Начальник отдела №2
полковник полиции А.Р. Фамильнов

Начальник сектора отдела №2
подполковник полиции И.М. Нурмухаметов

Старший научный сотрудник отдела №2 А.А. Клочков

Научный сотрудник отдела №2
лейтенант полиции Г.М. Дёмин



gost.e-ecolog.ru